OIPE IAP21
MAR 08 2006
PATENT & TRADEMARK OFFICE

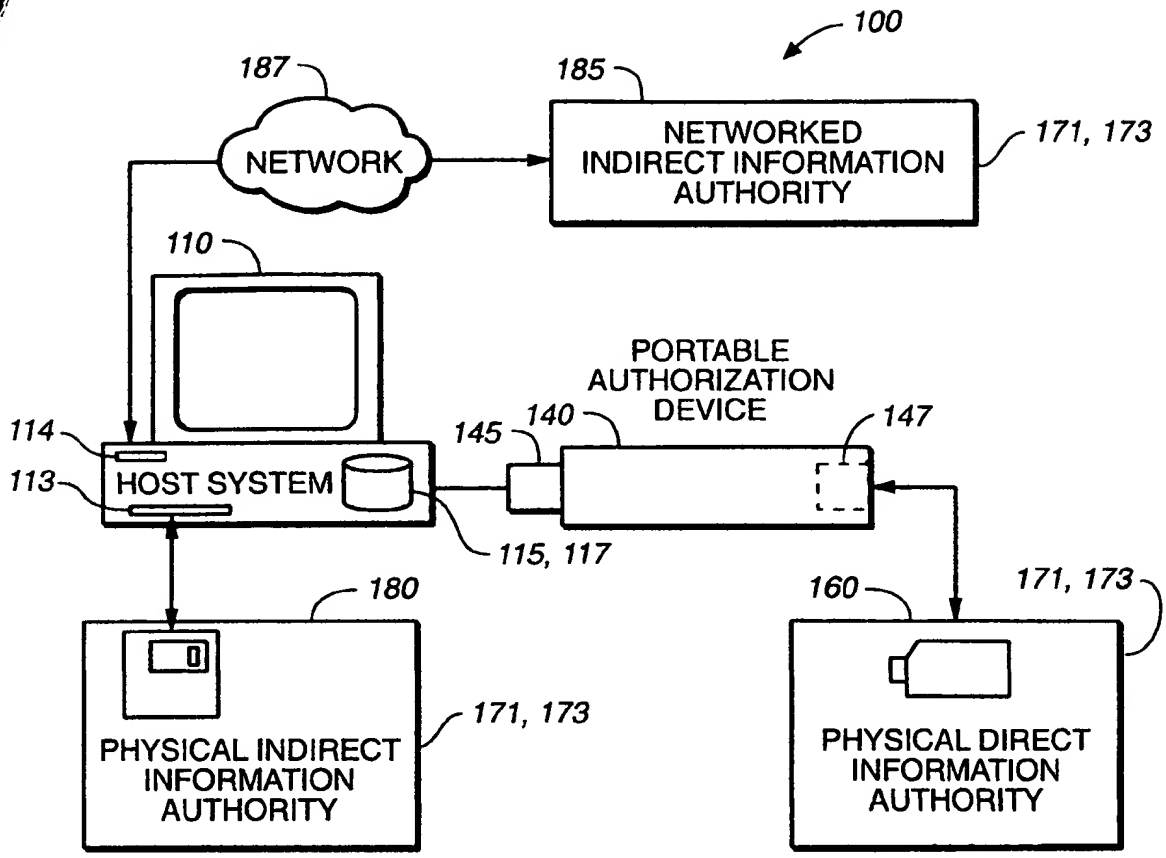

FIG._1

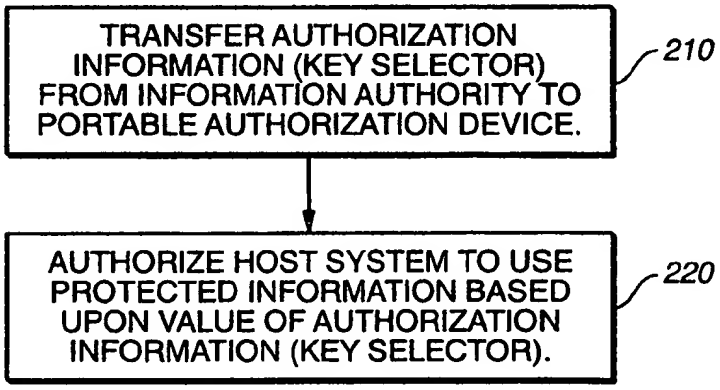

FIG._2

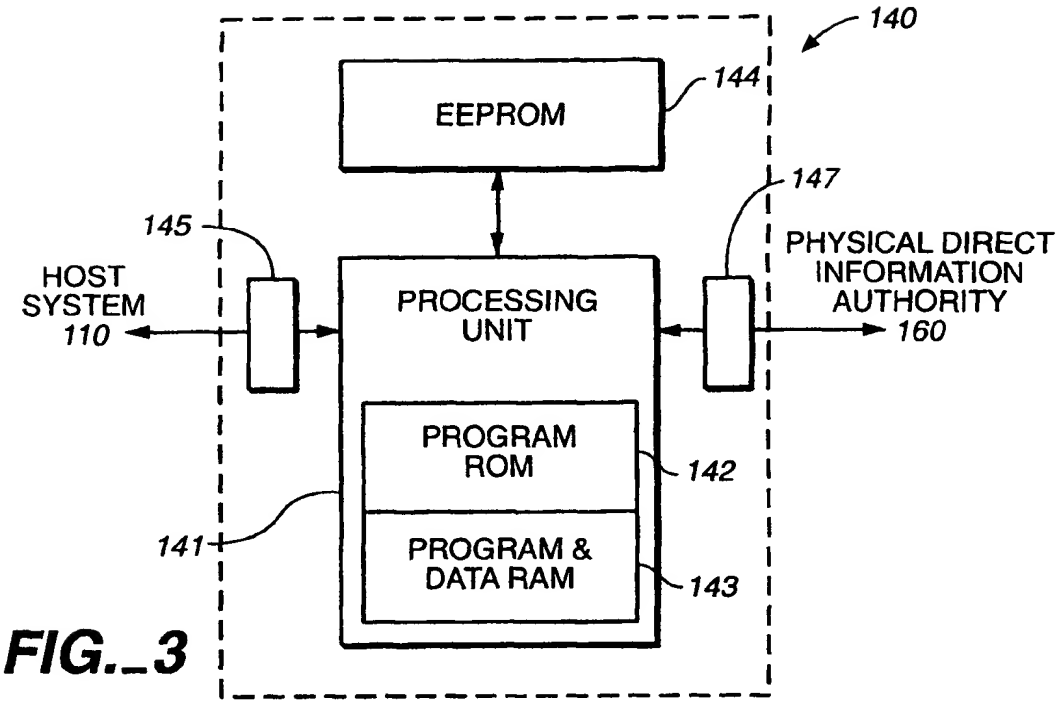
140
EEPROM
144
147
145
HOST
SYSTEM
110
PROCESSING
UNIT
PHYSICAL DIRECT
INFORMATION
AUTHORITY
160
PROGRAM
ROM
142
141
PROGRAM &
DATA RAM
143

FIG._3

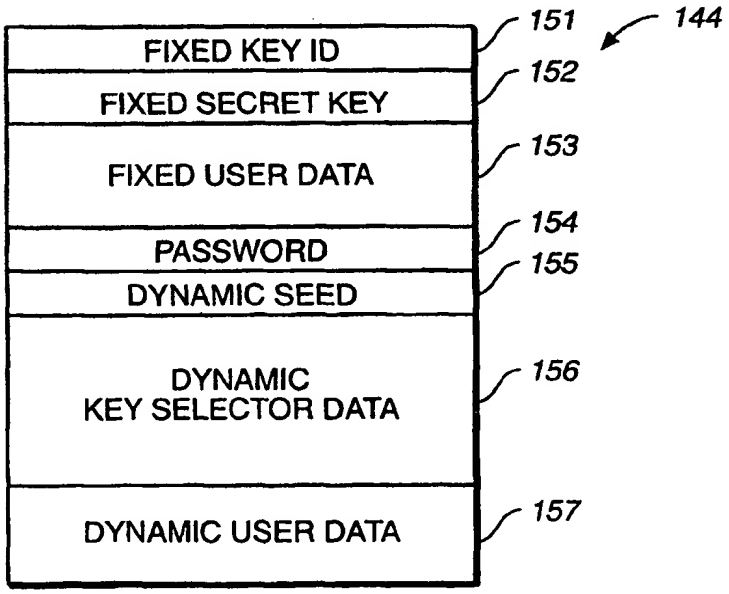
151
144
FIXED KEY ID
152
FIXED SECRET KEY
153
FIXED USER DATA
154
PASSWORD
155
DYNAMIC SEED
156
DYNAMIC
KEY SELECTOR DATA
157
DYNAMIC USER DATA

FIG._5

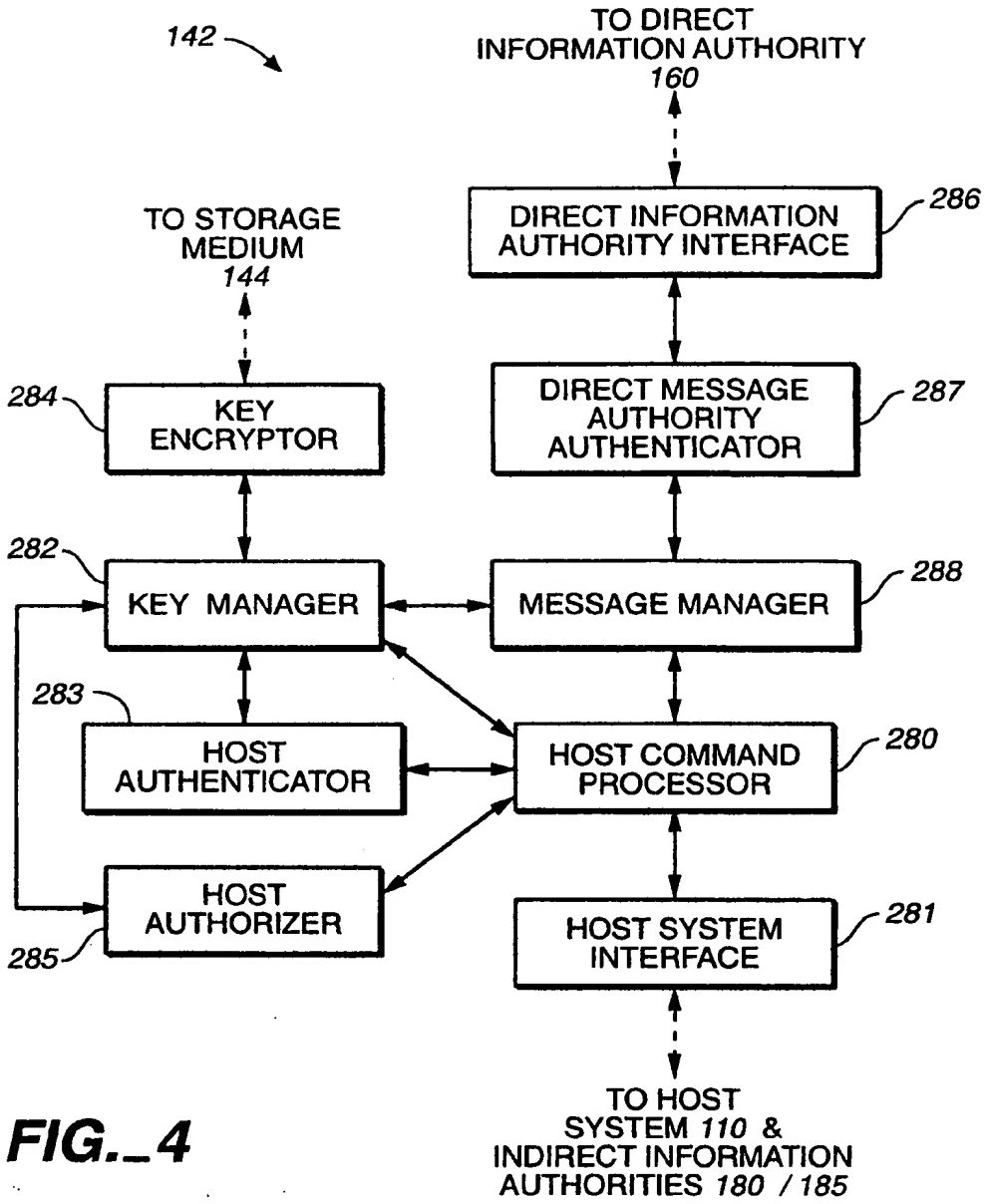
142
TO DIRECT INFORMATION AUTHORITY 160
TO STORAGE MEDIUM 144
DIRECT INFORMATION AUTHORITY INTERFACE
286
284
KEY ENCRYPTOR
DIRECT MESSAGE AUTHORITY AUTHENTICATOR
287
282
KEY MANAGER
MESSAGE MANAGER
288
283
HOST AUTHENTICATOR
HOST COMMAND PROCESSOR
280
HOST AUTHORIZER
285
HOST SYSTEM INTERFACE
281
TO HOST SYSTEM 110 & INDIRECT INFORMATION AUTHORITIES 180 / 185

FIG._4

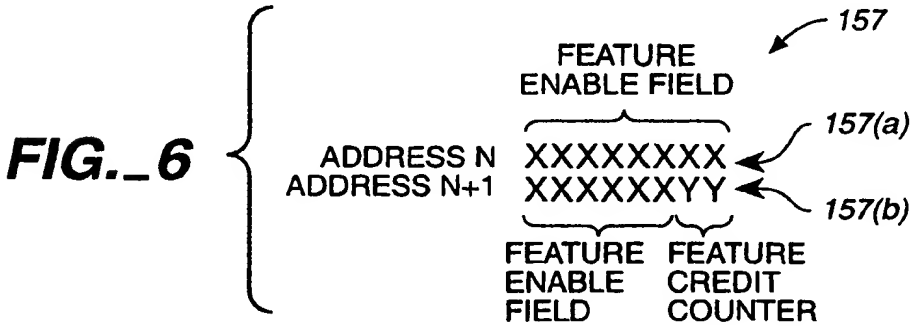
157
FEATURE ENABLE FIELD
157(a)
ADDRESS N XXXXXXXX
ADDRESS N+1 XXXXXXYY
157(b)
FEATURE ENABLE FIELD
FEATURE CREDIT COUNTER

FIG._6

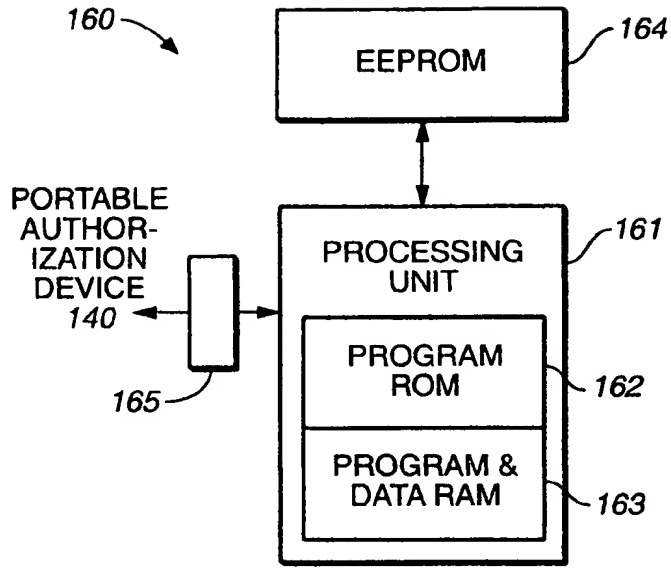

FIG._7

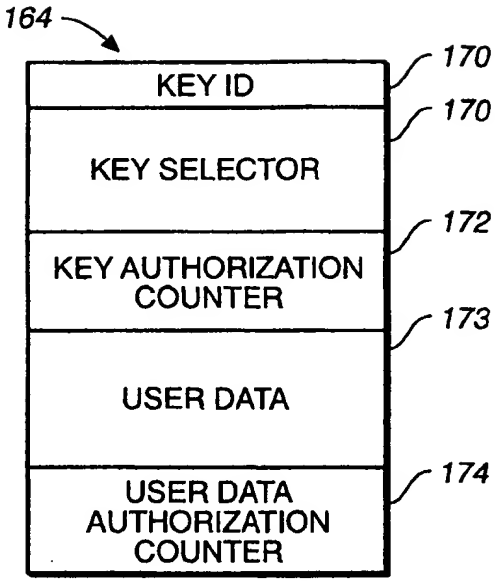

FIG._8

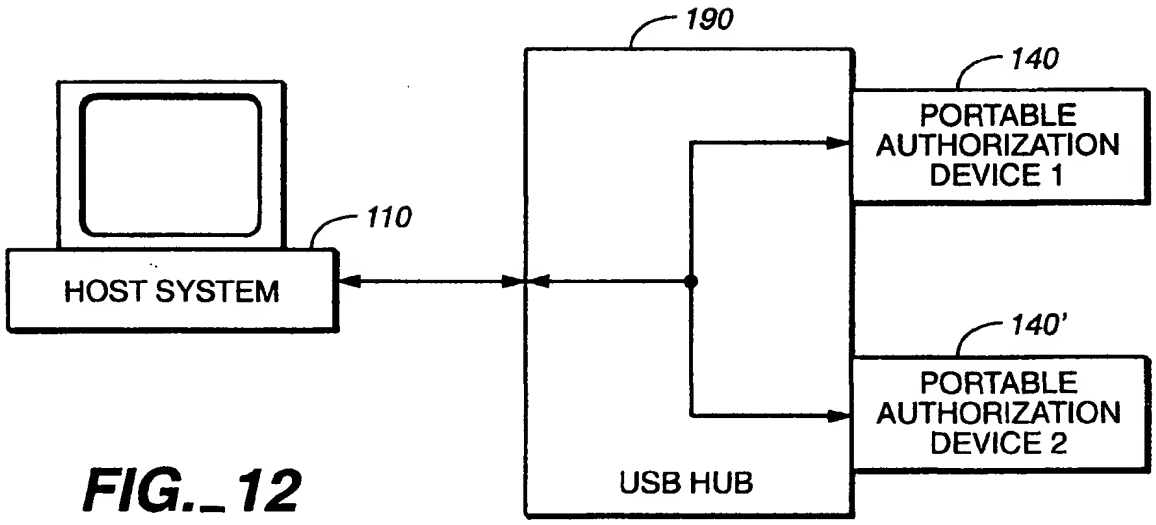

FIG._12

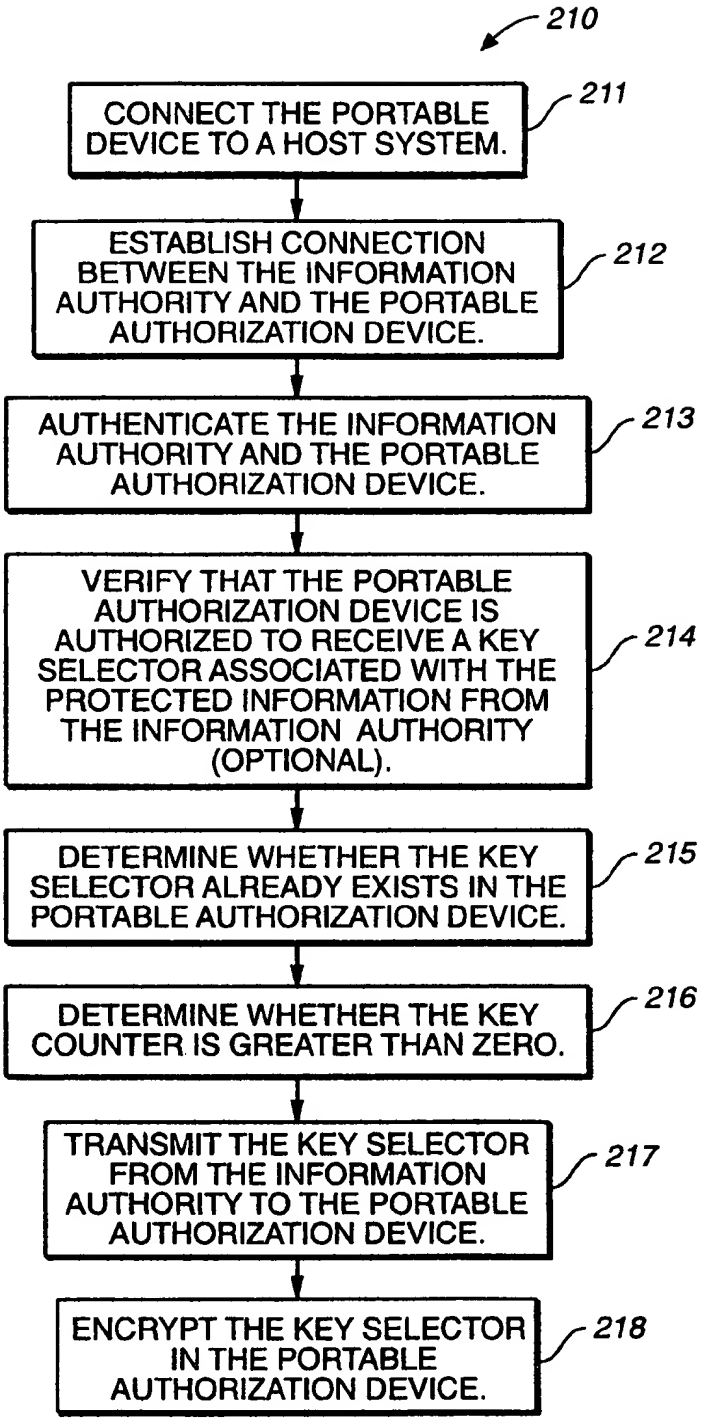
210
CONNECT THE PORTABLE DEVICE TO A HOST SYSTEM.
211
ESTABLISH CONNECTION BETWEEN THE INFORMATION AUTHORITY AND THE PORTABLE AUTHORIZATION DEVICE.
212
AUTHENTICATE THE INFORMATION AUTHORITY AND THE PORTABLE AUTHORIZATION DEVICE.
213
VERIFY THAT THE PORTABLE AUTHORIZATION DEVICE IS AUTHORIZED TO RECEIVE A KEY SELECTOR ASSOCIATED WITH THE PROTECTED INFORMATION FROM THE INFORMATION AUTHORITY (OPTIONAL).
214
DETERMINE WHETHER THE KEY SELECTOR ALREADY EXISTS IN THE PORTABLE AUTHORIZATION DEVICE.
215
DETERMINE WHETHER THE KEY COUNTER IS GREATER THAN ZERO.
216
TRANSMIT THE KEY SELECTOR FROM THE INFORMATION AUTHORITY TO THE PORTABLE AUTHORIZATION DEVICE.
217
ENCRYPT THE KEY SELECTOR IN THE PORTABLE AUTHORIZATION DEVICE.
218

FIG._9

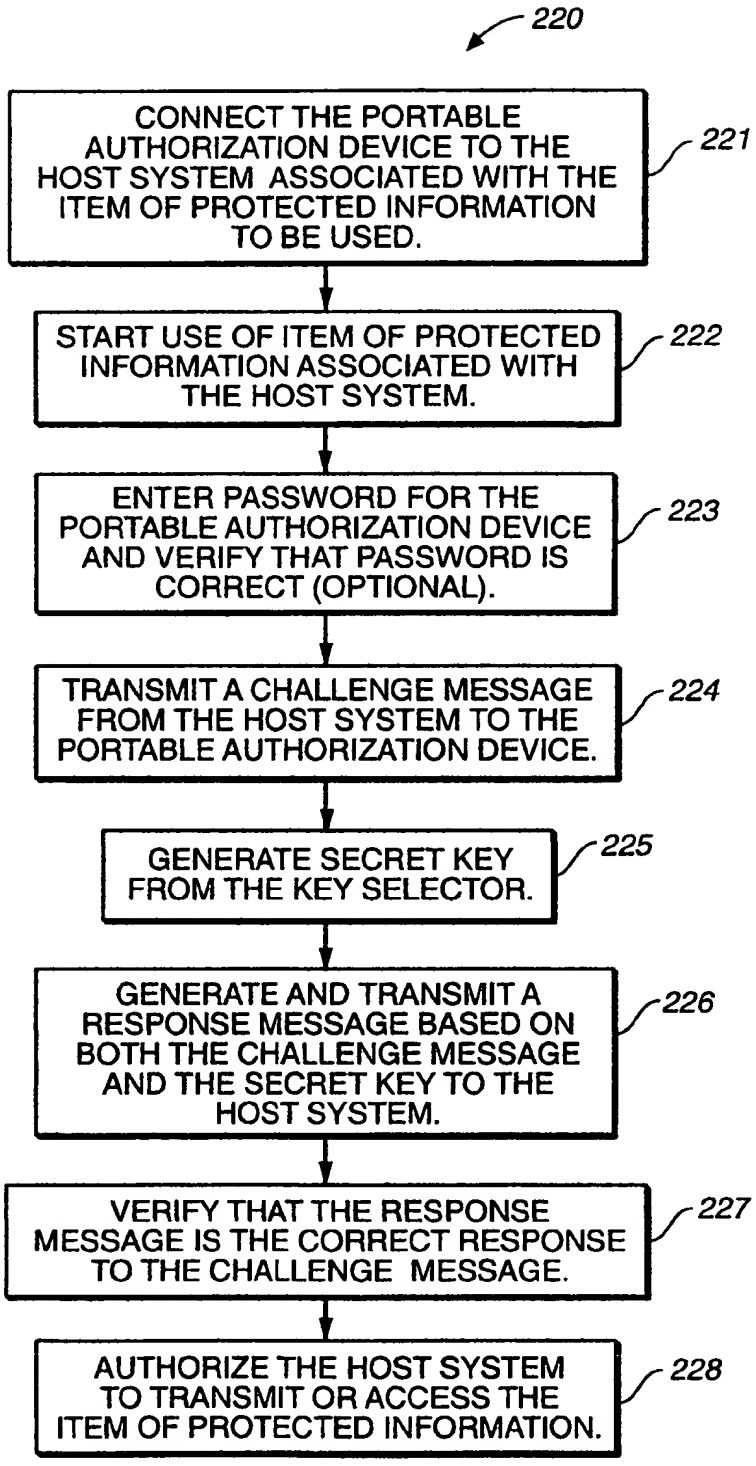
220
CONNECT THE PORTABLE AUTHORIZATION DEVICE TO THE HOST SYSTEM ASSOCIATED WITH THE ITEM OF PROTECTED INFORMATION TO BE USED.
221
START USE OF ITEM OF PROTECTED INFORMATION ASSOCIATED WITH THE HOST SYSTEM.
222
ENTER PASSWORD FOR THE PORTABLE AUTHORIZATION DEVICE AND VERIFY THAT PASSWORD IS CORRECT (OPTIONAL).
223
TRANSMIT A CHALLENGE MESSAGE FROM THE HOST SYSTEM TO THE PORTABLE AUTHORIZATION DEVICE.
224
GENERATE SECRET KEY FROM THE KEY SELECTOR.
225
GENERATE AND TRANSMIT A RESPONSE MESSAGE BASED ON BOTH THE CHALLENGE MESSAGE AND THE SECRET KEY TO THE HOST SYSTEM.
226
VERIFY THAT THE RESPONSE MESSAGE IS THE CORRECT RESPONSE TO THE CHALLENGE MESSAGE.
227
AUTHORIZE THE HOST SYSTEM TO TRANSMIT OR ACCESS THE ITEM OF PROTECTED INFORMATION.
228

FIG._10

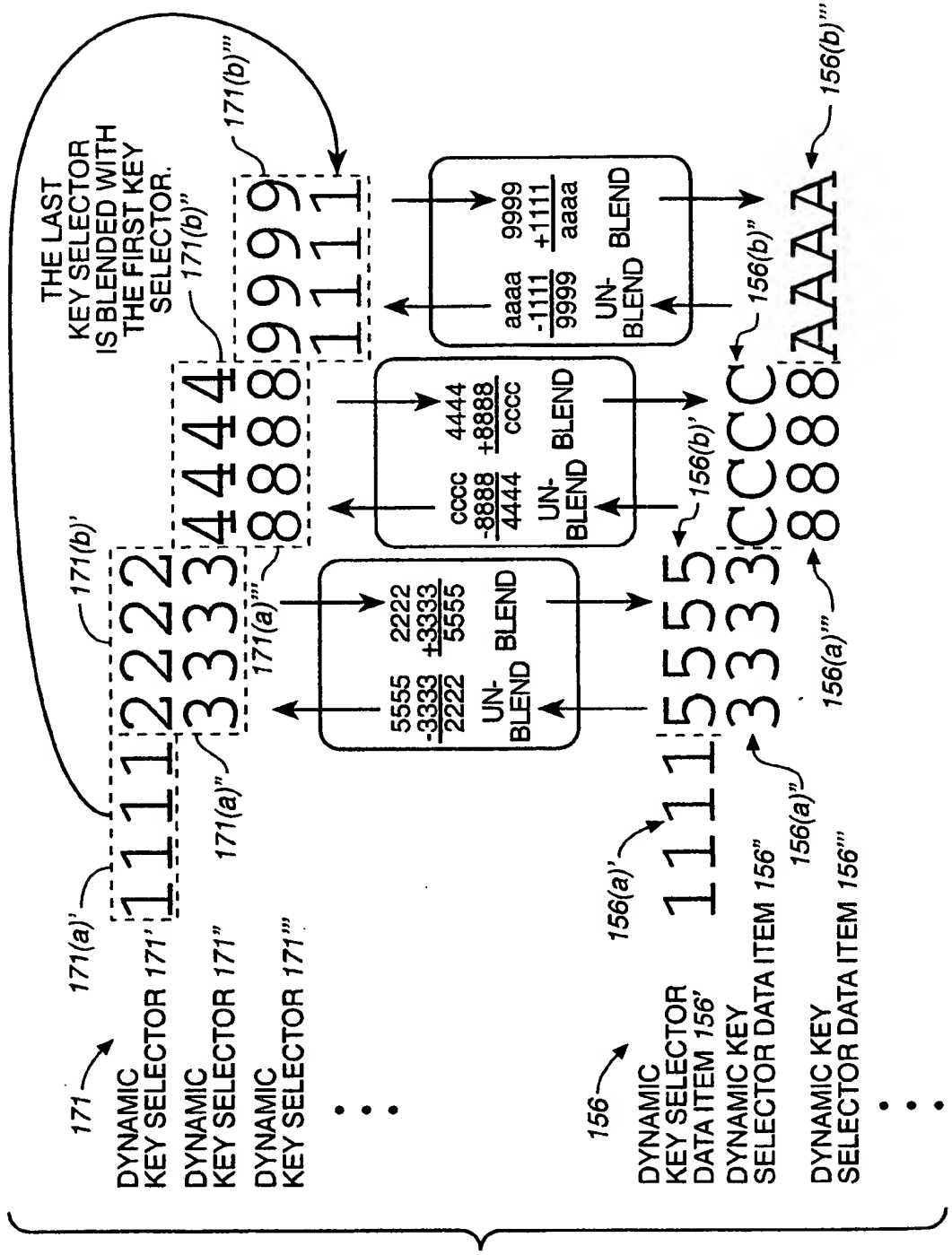
171
DYNAMIC KEY SELECTOR 171'
DYNAMIC KEY SELECTOR 171"
DYNAMIC KEY SELECTOR 171'"
171(a)'
171(b)'
171(a)"
171(b)"
171(a)'"
171(b)'"
THE LAST KEY SELECTOR IS BLENDED WITH THE FIRST KEY SELECTOR.
1111
2222
3333
4444
8888
9999
1111
5555 -3333 2222
2222 +3333 5555
UN-BLEND
BLEND
cccc -8888 4444
4444 +8888 cccc
aaaa -1111 9999
9999 +1111 aaaa
156
DYNAMIC KEY SELECTOR DATA ITEM 156'
DYNAMIC KEY SELECTOR DATA ITEM 156"
DYNAMIC KEY SELECTOR DATA ITEM 156'"
156(a)'
156(b)'
156(a)"
156(b)"
156(a)'"
156(b)'"
1111
5555
3333
CCCC
8888
AAAA

FIG._11